

JOeSandbox Cloud BASIC



ID: 433934

Sample Name: Pedido

N#U00famero 4432003039.exe

Cookbook: default.jbs

Time: 08:18:31

Date: 14/06/2021

Version: 32.0.0 Black Diamond


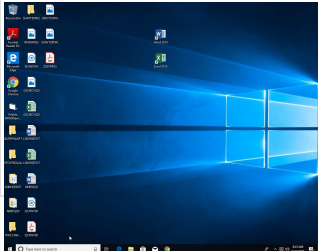
Table of Contents

Table of Contents	2
Analysis Report Pedido N#U00famer0 4432003039.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Signature Overview	3
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
Contacted IPs	7
General Information	7
Simulations	8
Behavior and APIs	8
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: Pedido N#U00famer0 4432003039.exe PID: 6236 Parent PID: 5720	10
General	10
Disassembly	10
Code Analysis	10






Analysis Report Pedido N#U00famero 4432003039.exe

Overview

General Information

Sample Name:	Pedido N#U00famero 4432003039.exe
Analysis ID:	433934
MD5:	d7c368f0c65c2a8..
SHA1:	0ff96bb6c163c9d..
SHA256:	439b1ce1850d9e..
Tags:	exe
Infos:	
Most interesting Screenshot:	
	

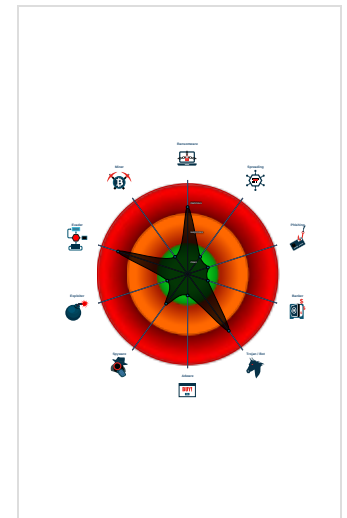
Detection

	
	
	
	
	
Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Potential malicious icon found
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Contains functionality to detect hard...
Detected RDTSC dummy instruction...
Found potential dummy code loops (...)
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to call native f...

Classification



Process Tree

- System is w10x64
-  Pedido N#U00famero 4432003039.exe (PID: 6236 cmdline: 'C:\Users\user\Desktop\Pedido N#U00famero 4432003039.exe' MD5: D7C368F0C65C2A8C565DF3815E70EF9E)
- cleanup

Malware Configuration

Threatname: GuLoader

<pre>{ "Payload URL": "https://andreameixeiro.com/karin_vJoQ5JCpNl6.bin" }</pre>
--

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.764314852.0000000002AD 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Networking:



C2 URLs / IPs found in malware configuration

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

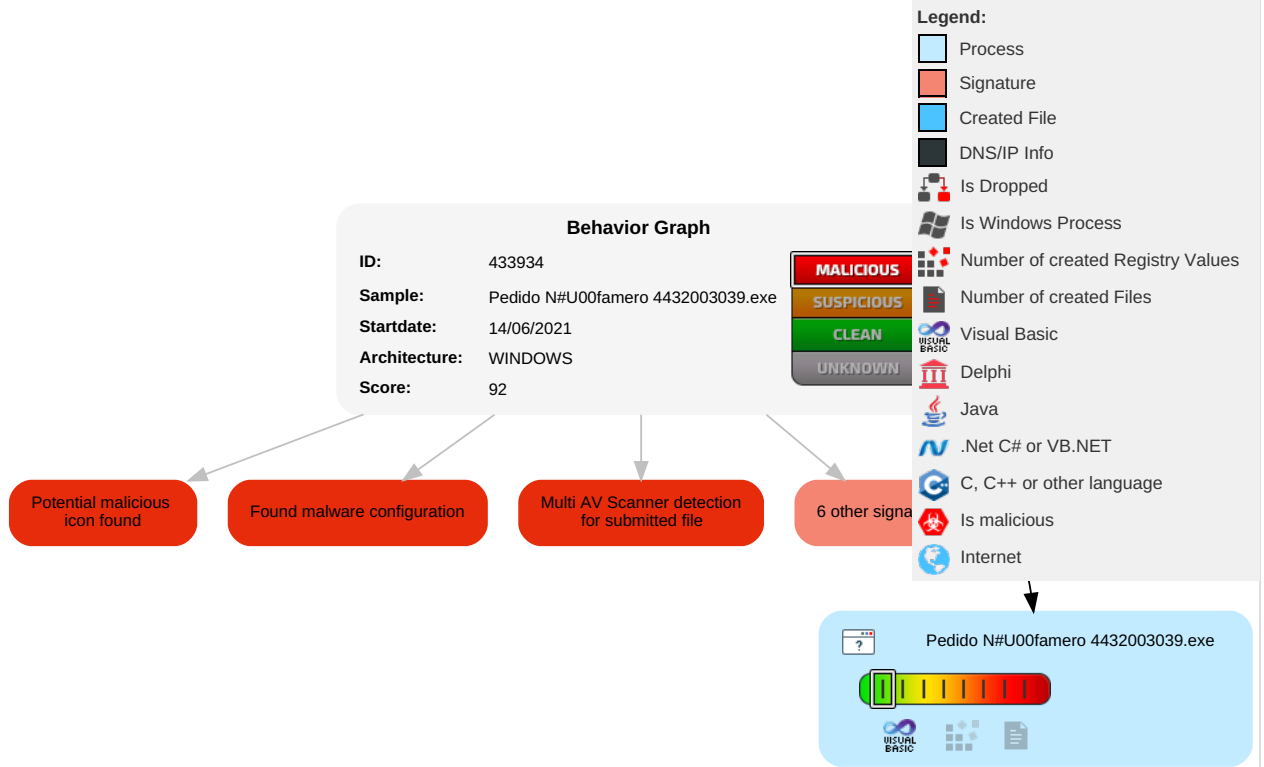


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Pedido N#U00famer0 4432003039.exe	50%	Virusotal		Browse
Pedido N#U00famer0 4432003039.exe	34%	Metadefender		Browse
Pedido N#U00famer0 4432003039.exe	62%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://andreameixeuro.com/karin_vJoQSJCpNI6.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://andreameixeueiro.com/karin_vJoQSJCpNI6.bin	true	<ul style="list-style-type: none">Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433934
Start date:	14.06.2021
Start time:	08:18:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pedido N#U00famero 4432003039.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none">HCA enabledEGA enabledHDC enabledAMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">Successful, ratio: 0.3% (good quality ratio 0.3%)Quality average: 50.2%Quality standard deviation: 2.2%
HCA Information:	<ul style="list-style-type: none">Successful, ratio: 52%Number of executed functions: 0Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSIFound application associated with file extension: .exeOverride analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations
Behavior and APIs
No simulations

Joe Sandbox View / Context
IPs
No context
Domains
No context
ASN
No context
JA3 Fingerprints
No context
Dropped Files
No context


Created / dropped Files
No created / dropped files found

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	3.8667127538435073
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) a (10002005/4) 99.15%Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%Generic Win/DOS Executable (2004/3) 0.02%DOS Executable Generic (2002/1) 0.02%Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Pedido N#U00famero 4432003039.exe
File size:	204800
MD5:	d7c368f0c65c2a8c565df3815e70ef9e
SHA1:	0ff96bb6c163c9dfc6f5e42c4407347c947dcb6c
SHA256:	439b1ce1850d9e816c22919cc13a412b9d1f00098486a642e97f34e7a62bd63a
SHA512:	05ff5aa7839f6ad1c9d004ce72ab20b51b1a844892694ab2124b11a52a165dad60e9020e91f14f7812371eccd26684585da349a27311636862b51809d2de0253
SSDEEP:	1536:JFNAAUuyxDI/795L+oJZzQwiVCw49ImWA6WWwdQxo:8ubh5LpJZzQRwxVWWwdQq

General

File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$......u...1..1. ..1.....0...~...0.....0..Rich1.....PE..L.....P.....h.....@.....
-----------------------	---

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x401368
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x50CD8DA9 [Sun Dec 16 09:00:25 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b2e3727c442d471988cc35e3702b319a

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2e6dc	0x2f000	False	0.217976022274	data	3.95853038654	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x30000	0xa7c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x31000	0x984	0x1000	False	0.177490234375	data	2.09868199866	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Pedido N#U00famero 4432003039.exe PID: 6236 Parent PID: 5720

General

Start time:	08:19:24
Start date:	14/06/2021
Path:	C:\Users\user\Desktop\Pedido N#U00famero 4432003039.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Pedido N#U00famero 4432003039.exe'
Imagebase:	0x400000
File size:	204800 bytes
MD5 hash:	D7C368F0C65C2A8C565DF3815E70EF9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.764314852.0000000002AD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis